FIG.1

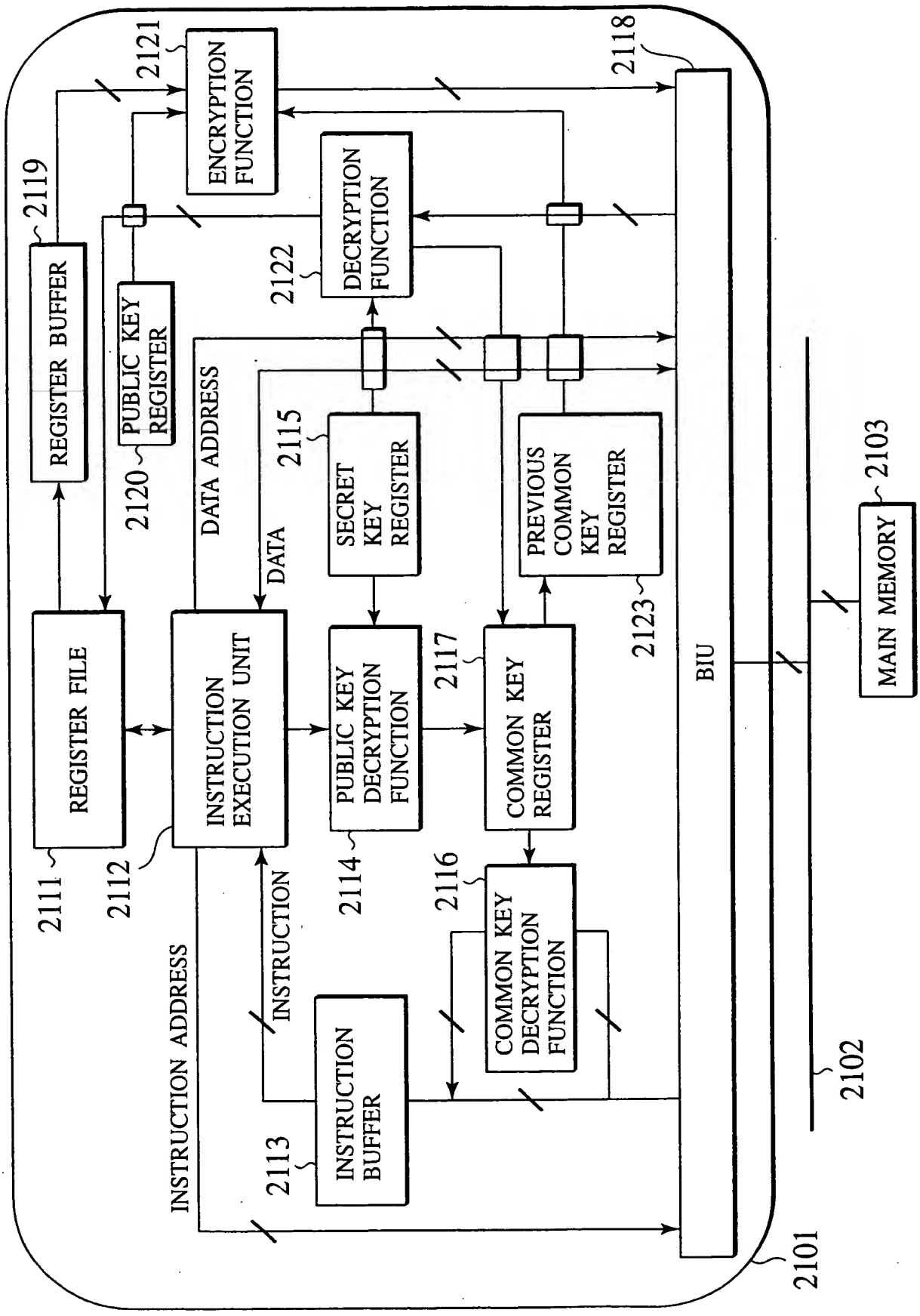

2101
2102
2103
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
REGISTER FILE
INSTRUCTION EXECUTION UNIT
INSTRUCTION BUFFER
PUBLIC KEY DECRYPTION FUNCTION
SECRET KEY REGISTER
COMMON KEY REGISTER
COMMON KEY DECRYPTION FUNCTION
PREVIOUS COMMON KEY REGISTER
REGISTER BUFFER
PUBLIC KEY REGISTER
ENCRYPTION FUNCTION
DECRYPTION FUNCTION
BIU
MAIN MEMORY
INSTRUCTION ADDRESS
INSTRUCTION
DATA ADDRESS
DATA

FIG.2

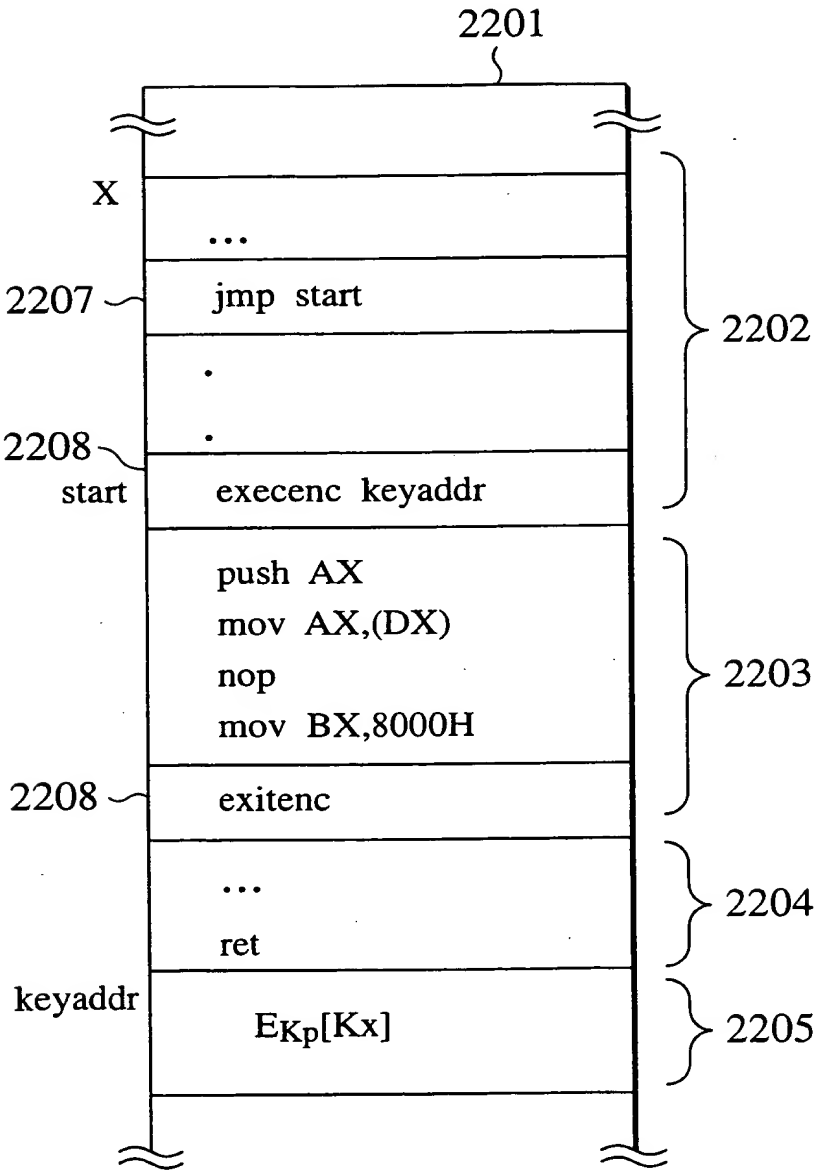
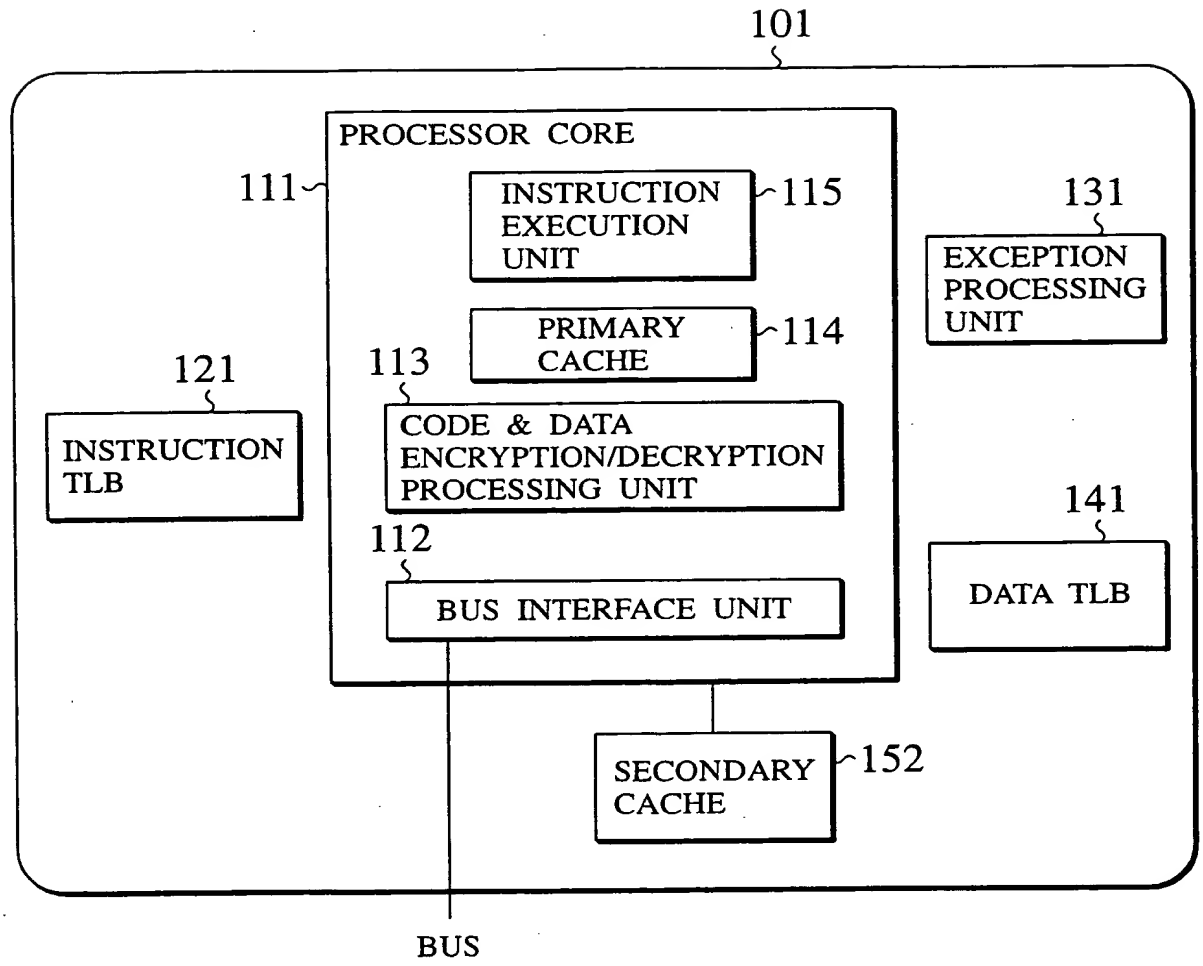

2201
X
...
2207
jmp start
2202
2208
start
execenc keyaddr
push AX
mov AX,(DX)
nop
mov BX,8000H
2203
2208
exitenc
...
ret
2204
keyaddr
$E_{Kp}[Kx]$
2205

FIG.3


101
PROCESSOR CORE
111
INSTRUCTION EXECUTION UNIT
115
PRIMARY CACHE
114
113
CODE & DATA ENCRYPTION/DECRYPTION PROCESSING UNIT
112
BUS INTERFACE UNIT
121
INSTRUCTION TLB
131
EXCEPTION PROCESSING UNIT
141
DATA TLB
SECONDARY CACHE
152
BUS

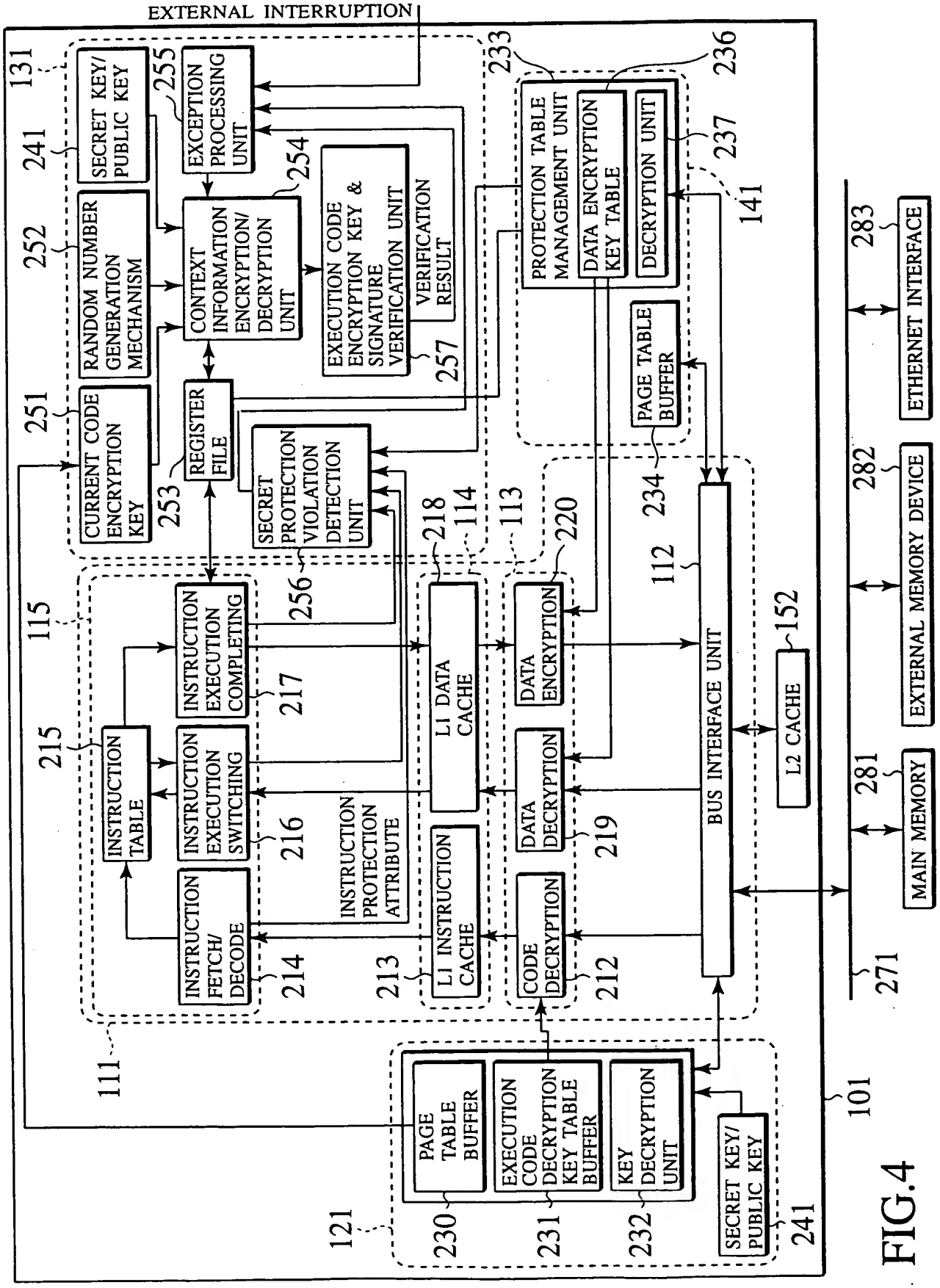
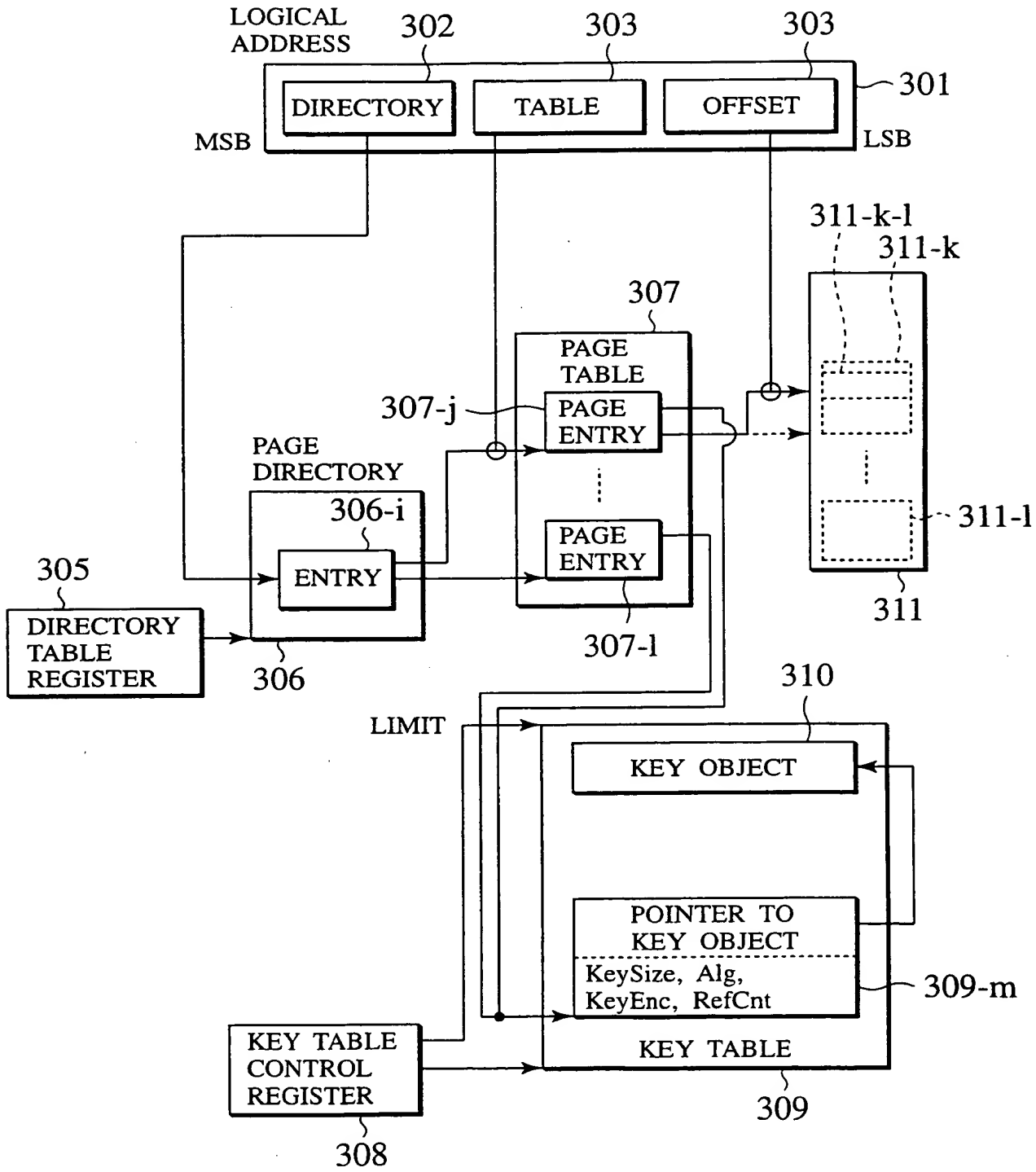

EXTERNAL INTERRUPTION
131
SECRET KEY/ PUBLIC KEY
255
EXCEPTION PROCESSING UNIT
241
252
RANDOM NUMBER GENERATION MECHANISM
CONTEXT INFORMATION ENCRYPTION/ DECRYPTION UNIT
254
EXECUTION CODE ENCRYPTION KEY & SIGNATURE VERIFICATION UNIT
VERIFICATION RESULT
257
233
PROTECTION TABLE MANAGEMENT UNIT
DATA ENCRYPTION KEY TABLE
DECRYPTION UNIT
236
237
141
283
ETHERNET INTERFACE
251
CURRENT CODE ENCRYPTION KEY
253
REGISTER FILE
SECRET PROTECTION VIOLATION DETECTION UNIT
PAGE TABLE BUFFER
234
218
114
113
220
112
256
115
INSTRUCTION EXECUTION COMPLETING
217
L1 DATA CACHE
DATA ENCRYPTION
152
L2 CACHE
282
EXTERNAL MEMORY DEVICE
215
INSTRUCTION TABLE
INSTRUCTION EXECUTION SWITCHING
216
INSTRUCTION PROTECTION ATTRIBUTE
DATA DECRYPTION
219
BUS INTERFACE UNIT
281
MAIN MEMORY
INSTRUCTION FETCH/ DECODE
214
213
L1 INSTRUCTION CACHE
CODE DECRYPTION
212
271
111
101
121
PAGE TABLE BUFFER
230
EXECUTION CODE DECRYPTION KEY TABLE BUFFER
231
KEY DECRYPTION UNIT
232
SECRET KEY/ PUBLIC KEY
241

FIG.4

FIG.5


LOGICAL ADDRESS
302
303
303
301
DIRECTORY
TABLE
OFFSET
MSB
LSB
311-k-l
311-k
307
PAGE TABLE
307-j
PAGE ENTRY
PAGE DIRECTORY
306-i
311-l
ENTRY
PAGE ENTRY
305
DIRECTORY TABLE REGISTER
306
307-l
311
310
LIMIT
KEY OBJECT
POINTER TO KEY OBJECT
KeySize, Alg, KeyEnc, RefCnt
309-m
KEY TABLE CONTROL REGISTER
KEY TABLE
309
308

6/15

FIG.6

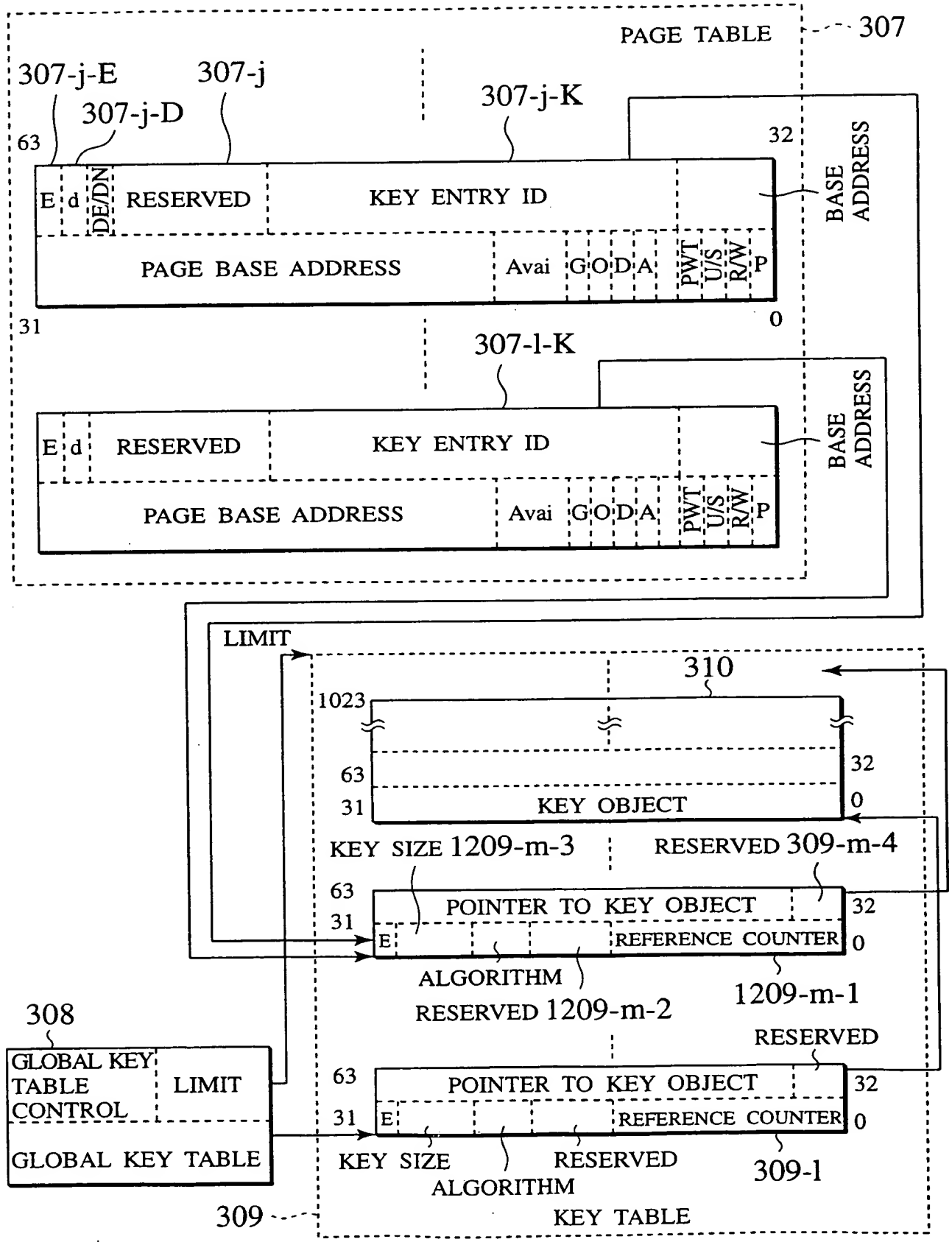

PAGE TABLE
307
307-j-E
307-j
307-j-D
307-j-K
63
32
E
d
DE/DN
RESERVED
KEY ENTRY ID
BASE ADDRESS
PAGE BASE ADDRESS
Avai
G
O
D
A
PWT
U/S
R/W
P
31
0
307-l-K
LIMIT
310
1023
63
32
31
0
KEY OBJECT
KEY SIZE 1209-m-3
RESERVED 309-m-4
POINTER TO KEY OBJECT
REFERENCE COUNTER
ALGORITHM
1209-m-1
RESERVED 1209-m-2
308
GLOBAL KEY TABLE CONTROL
LIMIT
GLOBAL KEY TABLE
RESERVED
POINTER TO KEY OBJECT
KEY SIZE
RESERVED
ALGORITHM
309-1
309
KEY TABLE

FIG.7A

	0	1	2	3
0	A0	A1	A2	A3
1	B0	B1	B2	B3
2	C0	C1	C2	C3
3	D0	D1	D2	D3
4	E0	E1	E2	E3
5	F0	F1	F2	F3
6	G0	G1	G2	G3
7	H0	H1	H2	H3

BEFORE INTERLEAVING

FIG.7B

0	A0	B0	C0	D0
1	E0	F0	G0	H0
2	A1	B1	C1	D1
3	E1	F1	G1	H1
4	A2	B2	C2	D2
5	E2	F2	G2	H2
6	A3	B3	C3	D3
7	E3	F3	G3	H3

AFTER INTERLEAVING

FIG.8

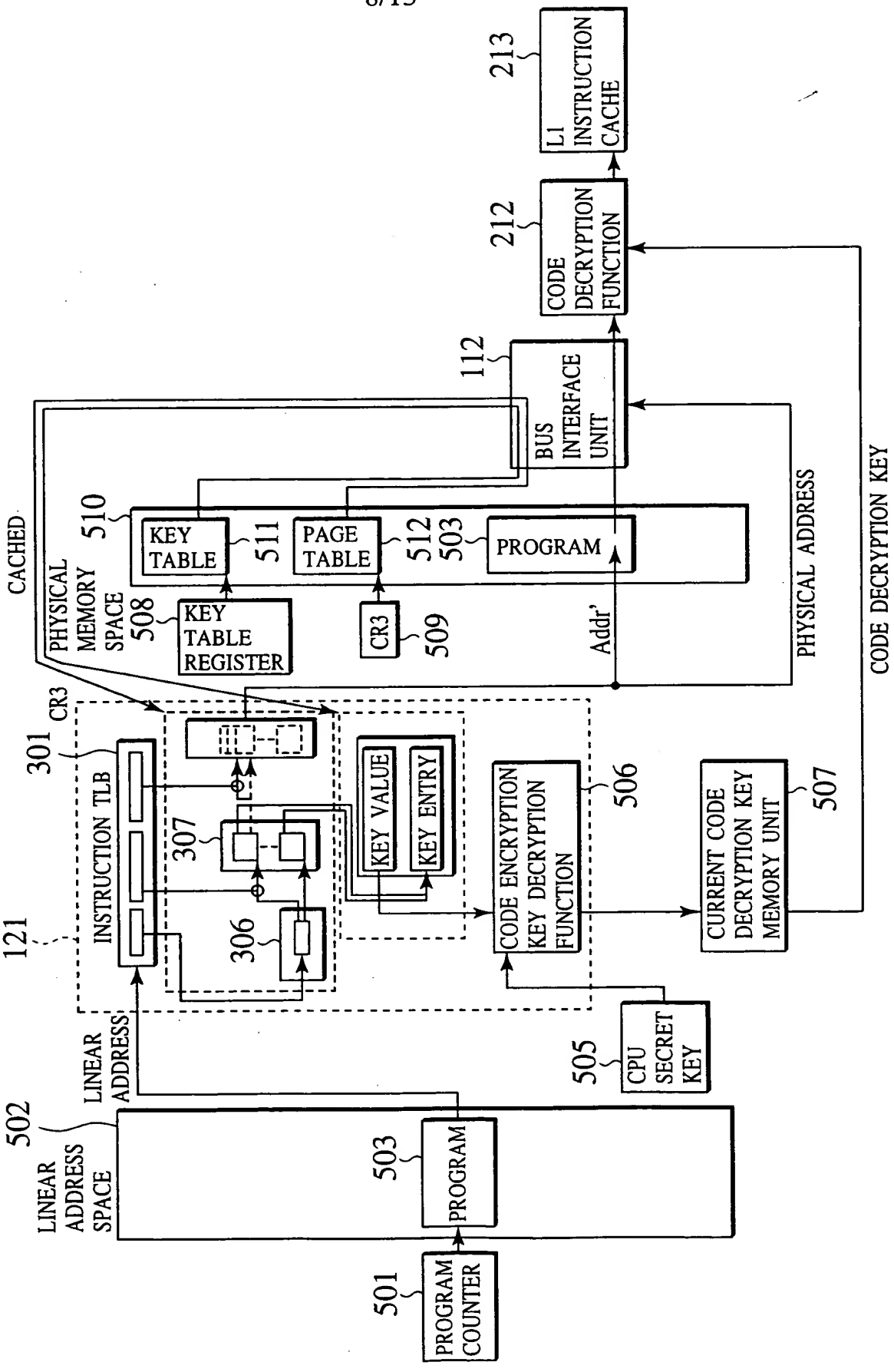

213
L1 INSTRUCTION CACHE
212
CODE DECRYPTION FUNCTION
112
BUS INTERFACE UNIT
CACHED
PHYSICAL MEMORY SPACE
510
KEY TABLE
511
PAGE TABLE
512
503
PROGRAM
508
KEY TABLE REGISTER
CR3
509
Addr'
PHYSICAL ADDRESS
CODE DECRYPTION KEY
CR3
301
INSTRUCTION TLB
307
KEY VALUE
KEY ENTRY
306
121
CODE ENCRYPTION KEY DECRYPTION FUNCTION
506
CURRENT CODE DECRYPTION KEY MEMORY UNIT
507
505
CPU SECRET KEY
LINEAR ADDRESS
502
LINEAR ADDRESS SPACE
503
PROGRAM
501
PROGRAM COUNTER

FIG.9

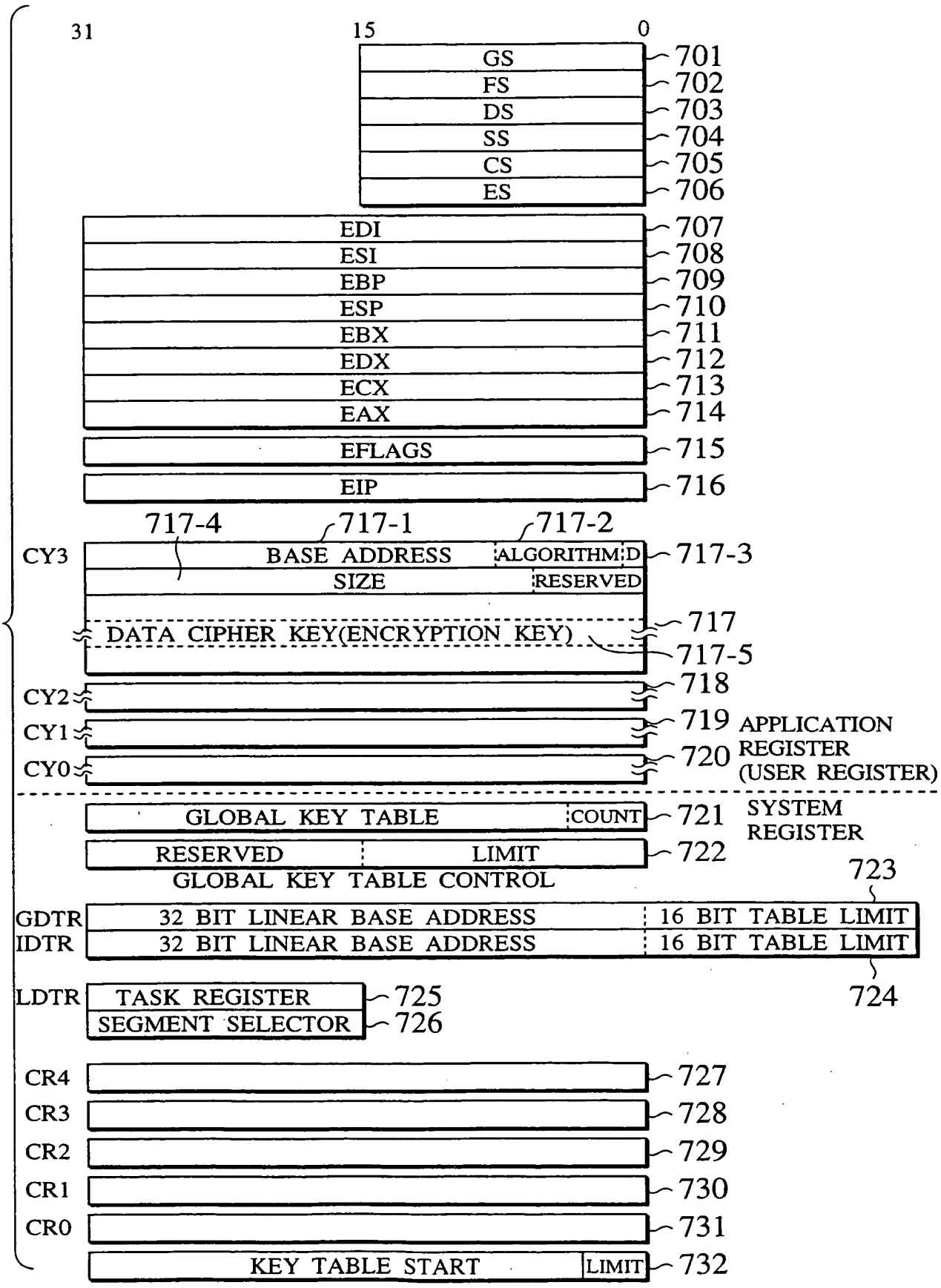

31
15
0
GS
FS
DS
SS
CS
ES
701
702
703
704
705
706
EDI
ESI
EBP
ESP
EBX
EDX
ECX
EAX
707
708
709
710
711
712
713
714
EFLAGS
715
EIP
716
717-4
717-1
717-2
CY3
BASE ADDRESS
ALGORITHM
D
717-3
SIZE
RESERVED
DATA CIPHER KEY(ENCRYPTION KEY)
717
717-5
CY2
718
CY1
719
CY0
720
APPLICATION REGISTER (USER REGISTER)
GLOBAL KEY TABLE
COUNT
721
SYSTEM REGISTER
RESERVED
LIMIT
722
GLOBAL KEY TABLE CONTROL
723
GDTR
32 BIT LINEAR BASE ADDRESS
16 BIT TABLE LIMIT
IDTR
32 BIT LINEAR BASE ADDRESS
16 BIT TABLE LIMIT
724
LDTR
TASK REGISTER
725
SEGMENT SELECTOR
726
CR4
727
CR3
728
CR2
729
CR1
730
CR0
731
KEY TABLE START
LIMIT
732

FIG.10

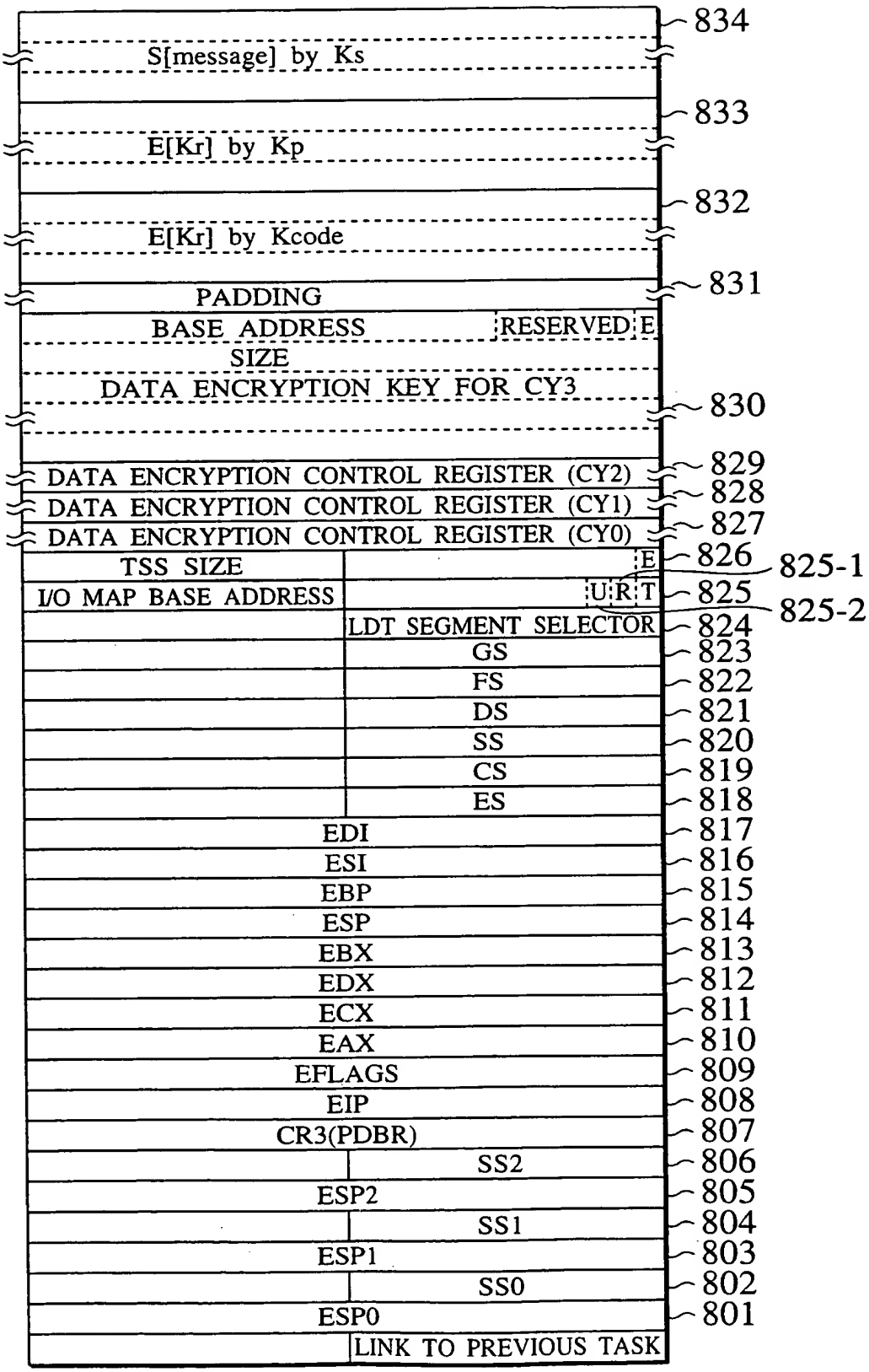

834
S[message] by Ks
833
E[Kr] by Kp
832
E[Kr] by Kcode
831
PADDING
BASE ADDRESS
RESERVED
E
SIZE
DATA ENCRYPTION KEY FOR CY3
830
DATA ENCRYPTION CONTROL REGISTER (CY2)
829
DATA ENCRYPTION CONTROL REGISTER (CY1)
828
DATA ENCRYPTION CONTROL REGISTER (CY0)
827
TSS SIZE
E
826
825-1
I/O MAP BASE ADDRESS
U
R
T
825
825-2
LDT SEGMENT SELECTOR
824
GS
823
FS
822
DS
821
SS
820
CS
819
ES
818
EDI
817
ESI
816
EBP
815
ESP
814
EBX
813
EDX
812
ECX
811
EAX
810
EFLAGS
809
EIP
808
CR3(PDBR)
807
SS2
806
ESP2
805
SS1
804
ESP1
803
SS0
802
ESP0
801
LINK TO PREVIOUS TASK

FIG.11

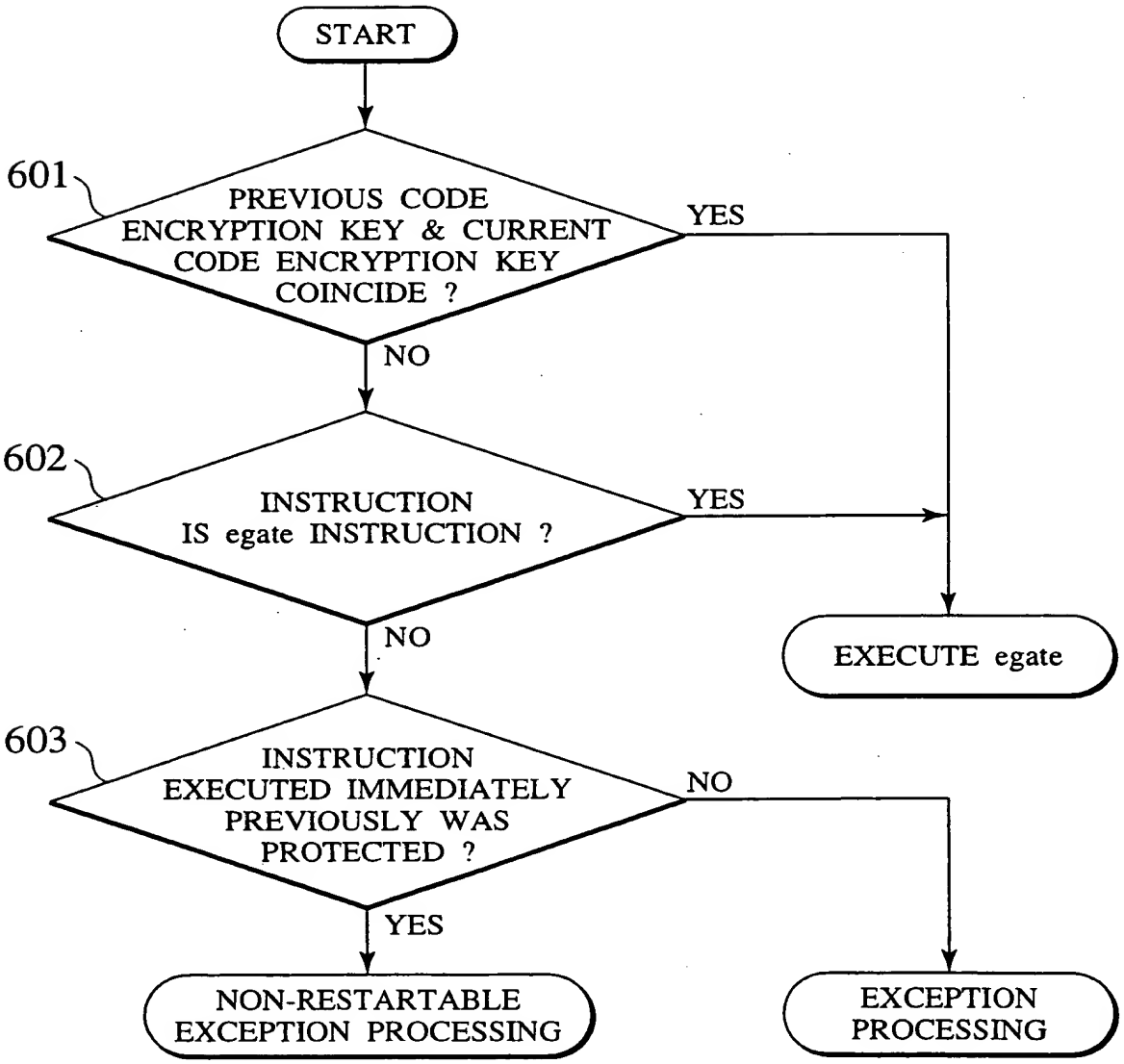

START
601
PREVIOUS CODE ENCRYPTION KEY & CURRENT CODE ENCRYPTION KEY COINCIDE ?
YES
NO
602
INSTRUCTION IS egate INSTRUCTION ?
YES
NO
EXECUTE egate
603
INSTRUCTION EXECUTED IMMEDIATELY PREVIOUSLY WAS PROTECTED ?
NO
YES
NON-RESTARTABLE EXCEPTION PROCESSING
EXCEPTION PROCESSING

FIG.12

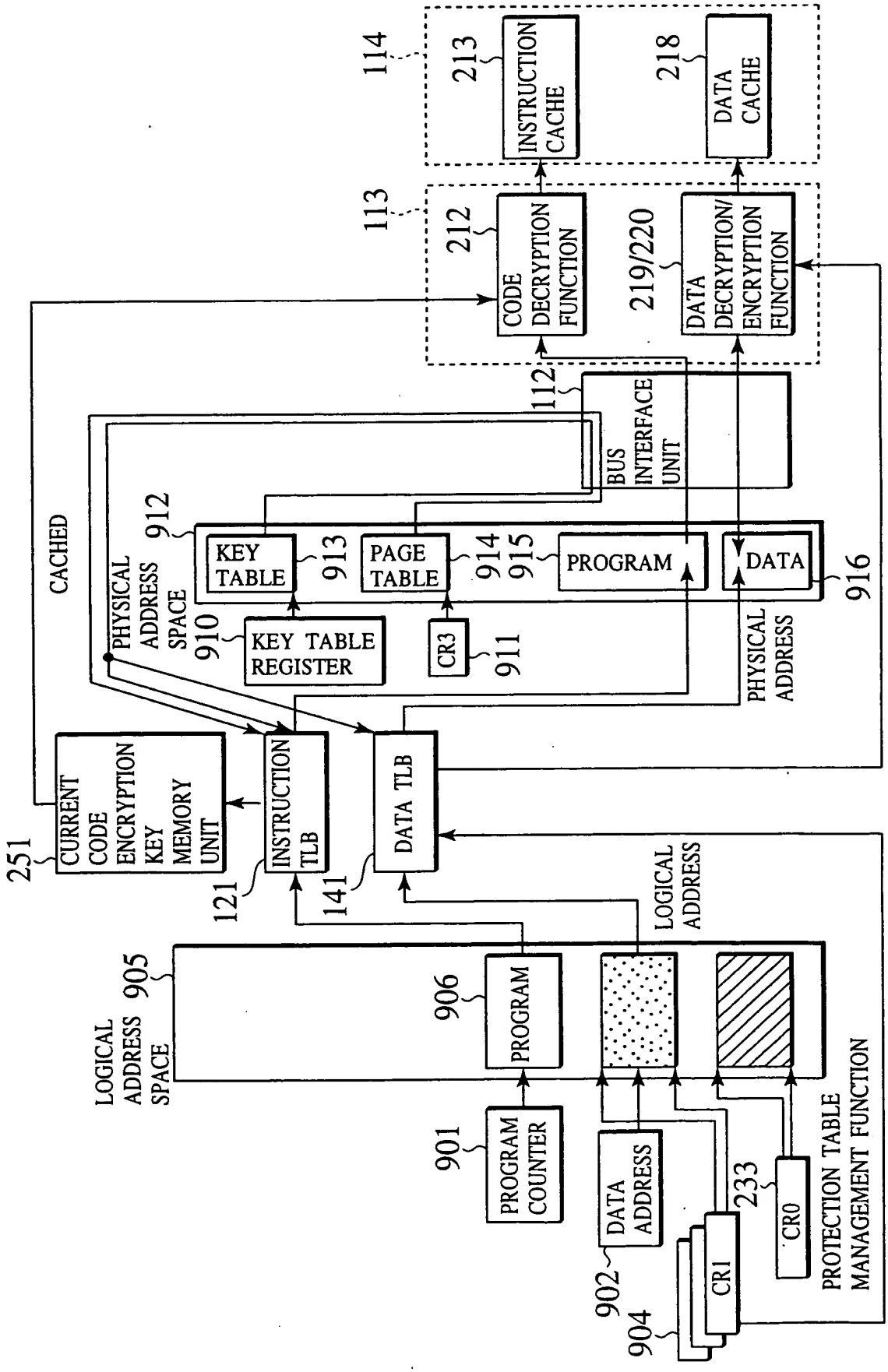

114
213
INSTRUCTION CACHE
218
DATA CACHE
113
212
CODE DECRYPTION FUNCTION
219/220
DATA DECRYPTION/ ENCRYPTION FUNCTION
112
BUS INTERFACE UNIT
CACHED
912
PHYSICAL ADDRESS SPACE
KEY TABLE
913
PAGE TABLE
914
915
PROGRAM
DATA
916
910
KEY TABLE REGISTER
CR3
911
PHYSICAL ADDRESS
251
CURRENT CODE ENCRYPTION KEY MEMORY UNIT
INSTRUCTION TLB
121
DATA TLB
141
LOGICAL ADDRESS
905
LOGICAL ADDRESS SPACE
906
PROGRAM
901
PROGRAM COUNTER
DATA ADDRESS
902
CR1
904
233
CR0
PROTECTION TABLE MANAGEMENT FUNCTION

FIG.13

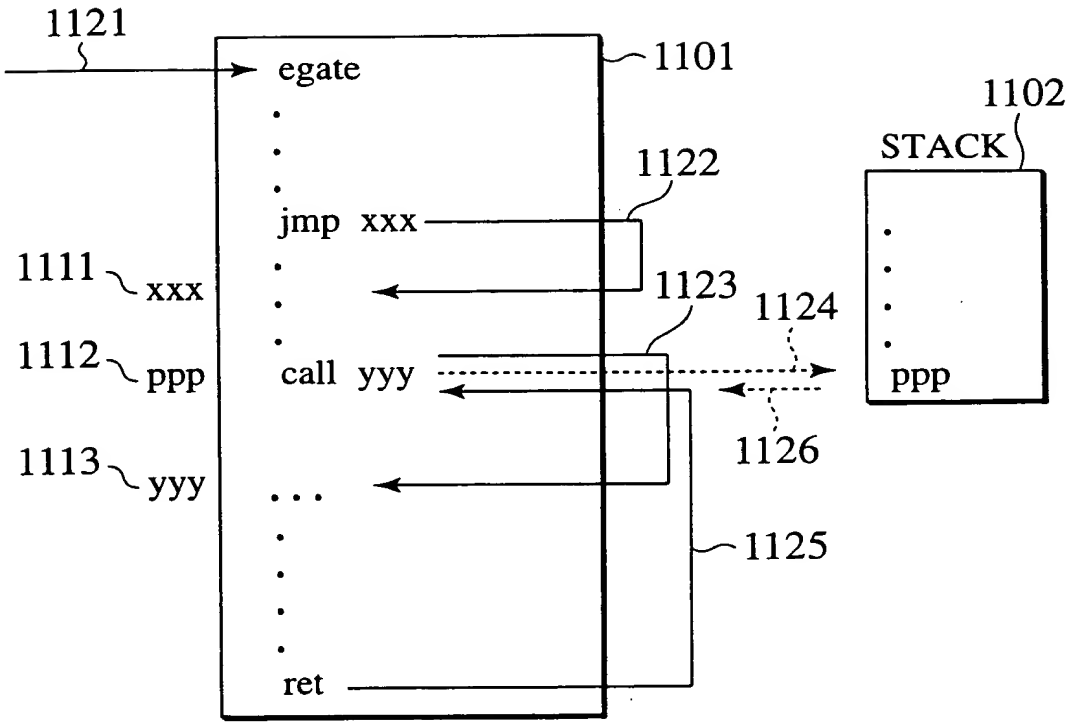

1121
egate
1101
1102
STACK
1122
jmp xxx
1111
xxx
1123
1124
1112
ppp
call yyy
ppp
1126
1113
yyy
1125
ret

FIG.14

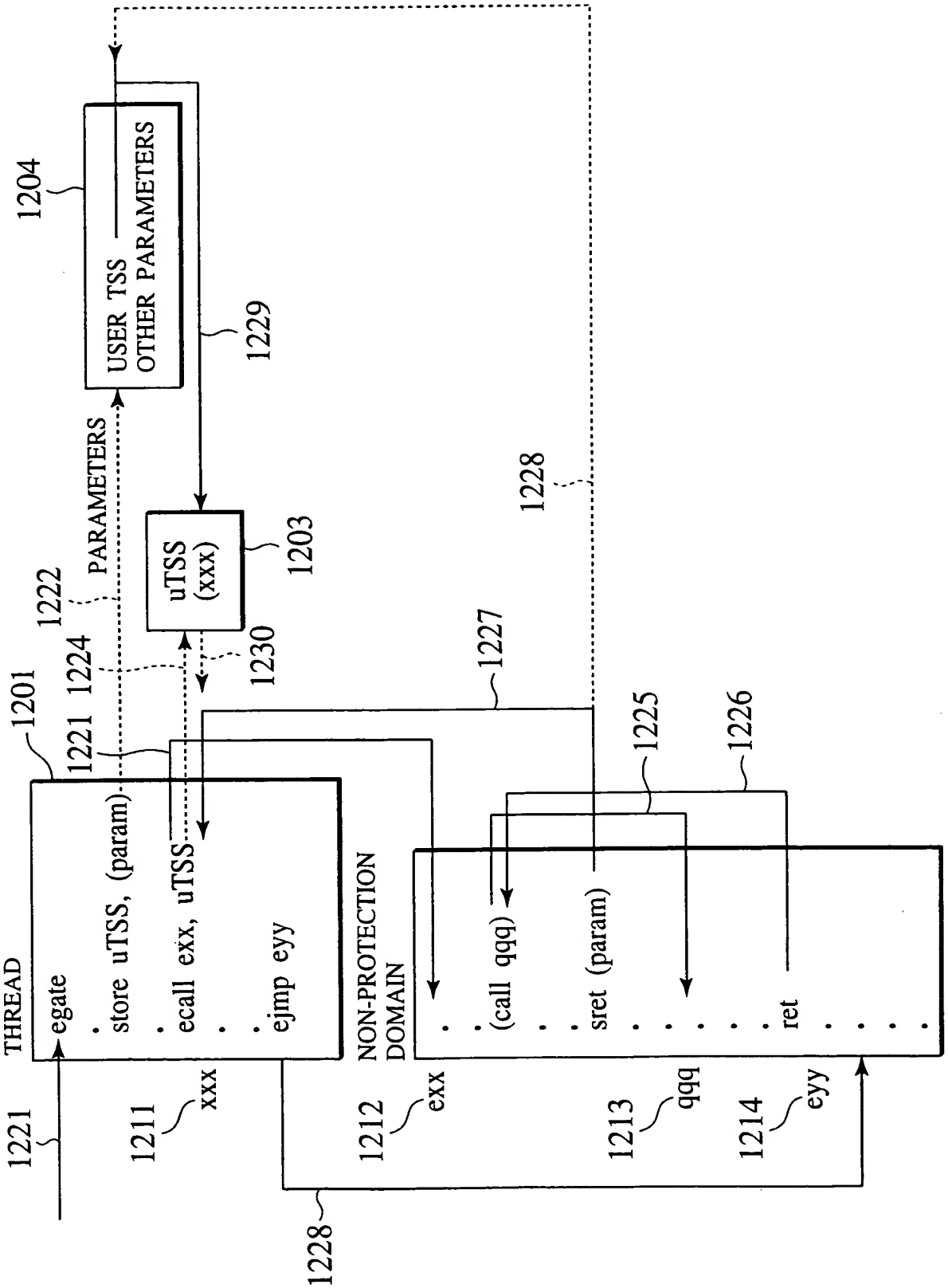

1204
USER TSS
OTHER PARAMETERS
1229
1228
PARAMETERS
1222
uTSS
(xxx)
1203
1224
1230
1227
1201
1221
1225
1226
THREAD
egate
store uTSS, (param)
ecall exx, uTSS
ejmp eyy
NON-PROTECTION
DOMAIN
(call qqq)
sret (param)
ret
1221
1211
xxx
1212
exx
1213
qqq
1214
eyy
1228

FIG.15
PRIOR ART

31	15	0	
I/O MAP BASE ADDRESS		T	100
	LDR SEGMENT SELECTOR		96
	GS		92
	FS		88
	DS		84
	SS		80
	CS		76
	ES		72
EDI			68
ESI			64
EBP			60
ESP			56
EBX			52
EDX			48
ECX			44
EAX			40
EFLAGS			36
EIP			32
CR3(PDBR)			28
	SS2		24
ESP2			20
	SS1		16
ESP1			12
	SS0		8
ESP0			4
	LINK TO PREVIOUS TASK		0